A robust watermarking scheme using sequency-ordered complex Hadamard transform

Aung, Aye; Ng, Boon Poh; Rahardja, Susanto

2010

Aung, A., Ng, B. P., & Rahardja, S. (2010). A Robust Watermarking Scheme Using Sequency-ordered Complex Hadamard Transform. Journal of Signal Processing Systems, 64, 319-333.

https://hdl.handle.net/10356/93997

https://doi.org/10.1007/s11265-010-0492-7

A Robust Watermarking Scheme Using Sequency-Ordered Complex Hadamard Transform

Aye Aung . Boon Poh Ng . Susanto Rahardja

Abstract This paper presents a robust phase watermarking scheme for still digital images based on the sequency-ordered complex Hadamard transform (SCHT). The transform matrix of the SCHT exhibits sequency ordering which is analogous to frequency in the discrete Fourier transform (DFT). Hence, sequency-based image analysis can be performed for image watermarking while providing simple implementation and with less computational complexity for computation of the transform. As the SCHT coefficients are complex numbers

A. Aung · B. P. Ng
School of Electrical and Electronic Engineering,
Nanyang Technological University, Singapore
639798 E-mail: aye aung@pmail.ntu.edu.sg,
ebpng@ntu.edu.sg S. Rahardja
Agency for Science, Technology, and Research (A*STAR),
Institute for Infocomm Research, Singapore 138632
E-mail: susantorahardja@ieee.org

which consist of both magnitudes and phases, they are suited to adopt phase modulation techniques to embed the watermark. In this proposed scheme, the phases of the SCHT coefficients in the sequency domain are altered to convey the watermark information using the phase shift keying (PSK) modulation. Low amplitude block selection (LABS) is used to enhance the imperceptibility of digital watermark, and amplitude boost (AB) method is employed to improve the robustness of the watermarking scheme. Spread spectrum (SS) technique is adopted to increase the security of watermark against various unintentional or intentional attacks. In order to demonstrate the effectiveness of the proposed watermarking scheme, simulations are conducted under various kinds of attacking operations. The results show that the proposed scheme is able to sustain a series of attacks including common geometric transformations such as scaling, rotating, cropping, painting, and common image-processing operations such as JPEG compression, low-pass filtering, sharpening, noising and phase perturbation, etc. Comparisons of the simulation results with the other schemes are also mentioned and the results reveal that the proposed scheme shows better robustness.

Keywords Phase Watermarking · Sequency-Ordered Complex Hadamard Transform (SCHT) · Spread Spectrum (SS) · Phase Shift Keying (PSK) · Low Amplitude Block Selection (LABS) · Amplitude Boost (AB)

1 Introduction

Due to the rapid and extensive development of high-speed internet and communication technologies, the use of multimedia applications is becoming more and more widespread. All the electronic documents are accessible to a large number of people in the world via the World Wide Web in a very cost-efficient way. Unfortunately, the digital information is quite easy to be duplicated and intentionally/unintentionally attacked by the unauthorized users. This motivates a significant interest for the researchers to find a way to discourage unauthorized copying and distributing of electronic documents, especially to protect the copyright. Consequently, digital watermarking emerges as one potential and popular solution to identify the copyright ownership and track the usage of digital multimedia works. By and large, a digital watermark is embedded in the digital data permanently to identify the source or ownership of the information.

In the literature, several methods have been developed for image watermarking. In general, they can be classified into two categories, one is processed in the spatial domain and the other in the transform domain. But the watermarks embedded in the spatial domain are not robust to tampering as compared to that concealed in the transform domain [1]. One major disadvantage of the spatial domain watermarking is that a common picutre cropping operation may deteriorate the watermark very easily [2]. On the other hand, the transform domain watermarking schemes have several desirable features. For example, one can insert the watermarks into the host image based on the

least perceptually significance of different transform coefficients. This will enhance the imperceptibility of the marks and lead to less visual degradation of the watermarked image. Besides, since the watermark is distributed over the transform coefficients irregularly, it is difficult for the attackers to remove the watermark. Various approaches have been introduced so far to transform the host image into the altered domain such as the discrete cosine transform (DCT) [2–4], the discrete Fourier transform (DFT) [5–8], the discrete wavelet transform (DWT) [8–10], the Walsh Hadamard transform (WHT) [11, 12], the unified complex Hadamard transform (UCHT) [12, 13], and the discrete fractional random transform (DFRNT) [1]. After transforming, the watermark is embedded using some robust algorithms. Finally, inverse transformation is performed to convert back to the spatial domain to obtain the watermarked images.

In [2], the transform domain approach is implemented based on the 8×8 block-based DCT. The DCT coefficients are altered to convey the watermark information. First, the watermark is generated as a binary pattern and then it is permuted to disperse the spatial relationship. It is pointed out in the paper that visually recognizable patterns used as watermarks are more intuitive to represent one's identity than a sequence of random numbers is. The scheme is able to sustain common image processing operations and JPEG compression. Ref. [11] utilized the WHT as the passage from spatial to frequency domain to embed the watermark due to its simplicity in implementation.

In order to enhance the robustness of watermarking schemes, phase modulation techniques in the transform domains are introduced in [5, 6, 12]. The reasons for selecting the phase components rather than the amplitudes are that a watermark embedded in the phase domain of the transform coefficients is more robust to tampering, and besides, it is well known from the communication theory that modulating the phase of the carrier can achieve better performance and superior noise immunity than amplitude modulation. The general approach in these papers is that the host image is segmented into the 8×8 blocks and each block is mapped into the transform domain. Only the portions which are most significant to the image integrity are marked. In [5], Chen et al. proposed the amplitude boost (AB) and the low amplitude block selection (LABS) methods to further enhance the robustness of the watermarking scheme. The phases of the selected DFT coefficients convey the binary watermark information. During the watermark extraction process, the original host image and the watermark are not needed, which corresponds to blind watermarking. The scheme achieves robustness which can sustain the JPEG compression and most common signal processing attacks, but it is vulnerable to the phase perturbation attack [14].

Falkowski [12] presented a new concept for a robust phase watermarking scheme using multi-polarity Walsh-Hadamard and Complex Hadamard Transform (CHT). In that paper, first, multiresolutional WHT is employed to decompose the host image into pyramid structure which consists of various bands to determine the most significant components of the image. Then, multi-

polarity CHT is performed on each selected 8×8 blocks. The phases of selected CHT coefficients are marked based on the pseudo-random watermark sequence and the coefficients of variance (COV) of the pixels in the 8×8 blocks before the CHT. This technique is robust to several attacks especially the JPEG lossy compression up to 10% quality factor. But two transformations (i.e., the WHT and the CHT) are required to do the watermarking. In [1], the DFRNT was used to propose a novel watermarking algorithm. In contrast to the previous methods listed above, the whole image is segmented into blocks only after the DFRNT. The blocks are chosen randomly for embedding according to the size of the watermark. Phase shift keying method is also adopted to reinforce the robustness of the watermarking scheme. It was found that it can sustain several attacks such as cropping, noising and low-pass filtering. Therefore, phase modulation techniques in the transform domains have a lot of good aspects in order to develop a robust watermarking algorithm.

This paper aims to propose a robust image watermarking algorithm which processes in the sequency domain using the sequency-ordered complex Hadamard transform [15]. The SCHT coefficients are the complex numbers consisting of both amplitudes and phases, hence, they are well suited to adopt phase shift keying methods to embed the watermark. Besides, the SCHT transformation is very simple as compared to the DFT with the availability of fast algorithms [16] since it is a complex Hadamard transform whose elements are confined to be four complex values $\{\pm 1, \pm j\}$. In addition, the transform matrix of the SCHT exhibits sequency ordering (analogous to frequency in the

DFT) which makes it possible to analyze the images using sequency-based image analysis (the analogy of frequency-based image analysis using the DFT) for watermark embedding. As such the watermark bits can be inserted into lower sequency components which are the most significant components of an image in order to increase the robustness of the watermarking scheme. In [17], the SCHT is employed in direct sequence CDMA systems as complex spreading sequences which are derived from the row vectors of an SCHT matrix due to their good crosscorrelation properties. In this paper, we introduce the SCHT in image watermarking to develop a robust watermarking technique. The embedding procedure is carried out in the sequency domain using the phase shift keying (PSK) method. The transform is based on the 8×8 image blocks. In our proposed scheme, two dimensional binary pattern watermark is used. First, the watermark is pre-permuted into noises to disperse the spatial relationship. Then, each watermark bit is expanded by spread spectrum and embedded by PSK modulation. This scheme also adopts the amplitude boost (AB) and low amplitude block selection (LABS) methods to further improve the robustness and to preserve the imperceptibility of the watermark.

The paper is organized as follows. In Section 2, we provide the basic definitions and properties of the SCHT. The proposed embedding algorithm is presented in Section 3. Section 4 describes the watermark extraction process. The experimental results are presented in Section 5, together with the simulation comparisons with the other schemes. Finally, this paper is concluded in Section 6.

2 Sequency-Ordered Complex Hadamard Transform

In this section, we shall provide a brief introduction to the SCHT [15]. Generally, SCHT is a discrete orthogonal transform with its transform matrix confined to four complex values $\{\pm 1, \pm j\}$. Any SCHT matrix of size $N \times N$ where $N = 2^n$ is generated from the complex Rademacher matrices whose row vectors are orthogonal to each other. The complex Rademacher matrices are the discrete versions of complex Rademacher functions (CRAD), and they are constructed by sampling the CRAD. The rth row of a complex Rademacher matrix of size $n \times 2^n$ is defined as

$$\mathbf{R}_n(r, k) = \mathrm{CRAD}(r, \frac{4k+1}{2^{n+2}}) \tag{1}$$

where r and k are the row and column indices, $r = 0, 1, \ldots, n-1$, $k = 0, 1, \ldots, 2^n - 1$, and CRAD is a complex Rademacher function with period 1. The CRAD can be expressed as

$$\mathrm{CRAD}(0, t) = \begin{cases} 1 & , t \in [0, \frac{1}{4}) \\ j & , t \in [\frac{1}{4}, \frac{1}{2}) \\ -1 & , t \in [\frac{1}{2}, \frac{3}{4}) \\ -j & , t \in [\frac{3}{4}, 1) \end{cases} \tag{2}$$

and

$$\mathrm{CRAD}(0, t+1) = \mathrm{CRAD}(0, t). \tag{3}$$

For non-negative integer r, $\mathrm{CRAD}(r, t)$ is defined as

$$\mathrm{CRAD}(r, t) = \mathrm{CRAD}(0, 2^r t) \tag{4}$$

where $r = 0, 1, 2, \ldots$. This means that $\mathrm{CRAD}(r, t)$ is obtained by compressing $\mathrm{CRAD}(0, t)$ in the horizontal direction by a factor of 2^r. Based on them the complex Rademacher matrices are generated as mentioned in (1). With the complex Rademacher matrices defined, Sequency-ordered Complex Hadamard Transform matrices, $\mathbf{H}_N$, are constructed as follows:

$$\mathbf{H}_N(m, k) = \prod_{r=0}^{n-1} \mathbf{R}_n(r, k)^{b_r} \tag{5}$$

where $\mathbf{R}_n(r, k)$ is the (rth, kth) element of the complex Rademacher matrix,

$$m = b_{n-1}2^{n-1} + \ldots + b_1 2^1 + b_0 2^0 \tag{6}$$

and $b_r = 0$ or 1. Let $\mathbf{R}_n(r)$, for $r = 0, 1, \ldots, n-1$, be the rth row vector of the complex Rademacher matrix, and also, let $\odot$ be the operator for element by element vector multiplication. For example, $\mathbf{H}_8(7, k)$ can be expressed as

$$\mathbf{H}_8(7, k) = \mathbf{R}_3(2, k) \odot \mathbf{R}_3(1, k) \odot \mathbf{R}_3(0, k). \tag{7}$$

Since binary number of 7_{10} is 111_2 and the row indices $2, 1$ and 0 refer to ones found in the binary bit positions.

Sequency Property: An SCHT matrix is a matrix whose row vectors are ordered in ascending number of sequencies. Each element of the SCHT matrix can be mapped to the unit circle of a complex plane to visualize the concept of sequency. Sequency describes the number of times that the row vector of a matrix crosses the imaginary axis in the unit circle of a complex plane over a normalized time base $0 \leq t \leq 1$ [18]. This is analogous to frequency in the

DFT where the Fourier components are arranged in an increasing harmonic number in terms of sine and cosine waves. In fact, with such property, the SCHT can be used as a tool for signal and image analysis [15].

Definition 1: An SCHT matrix of order $N \times N$, $\mathbf{H}_N$, is a square matrix and it is said to be orthogonal in the complex domain as

$$|\det \mathbf{H}_N| = N^{\frac{N}{2}} \tag{8}$$

and

$$\mathbf{H}_N \mathbf{H}_N^* = \mathbf{H}_N^* \mathbf{H}_N = N\mathbf{I}_N \tag{9}$$

where $\mathbf{H}_N^*$ is the complex conjugate transpose of $\mathbf{H}_N$ and $\mathbf{I}_N$ is the identity matrix of order $N = 2^n$.

Definition 2: The SCHT of a signal vector
$\mathbf{x}_N = [x(0), x(1), \ldots, x(N-1)]^T$ is defined as

$$\mathbf{X}_N = \frac{1}{N} \mathbf{H}_N^* \mathbf{x}_N \tag{10}$$

where $\mathbf{X}_N = [X(0), X(1), \cdots, X(N-1)]^T$ is the transformed complex column vector. The data sequence can be recovered uniquely from the inverse transform, that is,

$$\mathbf{x}_N = \mathbf{H}_N \mathbf{X}_N. \tag{11}$$

A two dimensional (2-D) SCHT of the segmented image block $N \times N$ can be performed by applying one dimensional SCHT on the rows of the block

followed by the corresponding columns. The 2-D SCHT is defined as

$$\mathbf{Y}_N = \mathbf{C}_N \mathbf{Z}_N \mathbf{C}_N^T \tag{12}$$

where $\mathbf{C}_N^T$ represents the transpose of $\mathbf{C}_N$,

$$\mathbf{C}_N = \frac{1}{\sqrt{N}} \mathbf{H}_N^* \tag{13}$$

where $\mathbf{H}_N^*$ is the complex conjugate transpose of the SCHT matrix $\mathbf{H}_N$, $\mathbf{Z}_N$ is the $N \times N$ real image block, and $\mathbf{Y}_N$ is the 2-D SCHT coefficient matrix of dimension $N \times N$. The SCHT coefficients of a real image are the complex values which consist of both magnitudes and phases, hence, PSK modulation can be utilized to embed the watermark in the SCHT transformed images.

3 Watermark Embedding Algorithm

The design and implementation of a novel transform domain based watermarking algorithm for grey-scaled images is presented in this section. A robust watermarking scheme must sustain all kinds of attacks, plus it should preserve the visual quality of the original image after embedding the watermark. Various methods are employed to improve the performance of our watermarking scheme. The overall watermarking procedure to conceal the watermark is shown in Fig. 1. The proposed scheme is outlined step by step as follows:

1. At first, the 2-D binary pattern watermark, $\mathbf{W}$, is scrambled into noise-liked pattern, $\mathbf{W}_p$, by applying pseudo-random permutation using a random sequence (PN_1) to disperse the spatial relationship and to enhance

the security. We use a visible image of 32×32 pixels as the watermark to be embedded. Such kinds of visually recognizable patterns are more natural to represent one's identity than a sequence of random numbers [2].

2. It is then transformed into a bipolar bit sequence and expanded by spread spectrum to become a spread bipolar bit sequence m.
3. On the other hand, the 8-bit grey-scaled image of 512×512 pixels is evenly divided into the 8×8 non-overlapping blocks.
4. The 2-D SCHT is performed for each 8×8 image block to transform the whole image from the spatial domain into the sequency domain.
5. Low amplitude block selection (LABS) strategy [5] is adopted in our watermarking scheme in order to preserve the imperceptibility of the watermark as much as possible. LABS selects a certain number of blocks, $\mathbf{B}_i$, which is equal to the length of the watermark bit sequence m as each secret bit is to be inserted into each transformed 8×8 block.
6. Subsequently, amplitude boost (AB) [5] is hired to enhance the robustness. The amplitude, A, of each selected SCHT coefficient, $Ae^{j\phi}$, from each selected block, $\mathbf{B}_i$, is raised to A' to combat the attacks.
7. The phase, ϕ, of each selected coefficient is altered to ϕ' according to the bipolar watermark bit sequence using PSK modulation. The embedding procedure is repeated for each secret bit in m until we get $\mathbf{Y}'$.
8. Finally, the inverse 2-D SCHT is performed on the transformed image $\mathbf{Y}'$ to obtain the respective watermarked image, $\mathbf{R}$.

The details of some steps are presented in the following.

3.1 Pseudo-random Permutation of the Watermark

In our approach, the watermark image is pre-permuted into noises using a pseudo-random sequence (PN_1 which will be kept for watermark extraction process in future) for the security purpose. The shape of the watermark becomes chaotic after permuting the image matrix as shown in Fig. 2. Hence, it will protect the watermark from being stolen by the others. The permutation is performed as follows:

1. First, transform the binary $M \times M$ watermark, $\mathbf{W}$, into a binary bit sequence, $\mathbf{u}_w$, of the size $1 \times n_w$ where $n_w = M \times M$.
2. Generate a sequence of indices (PN_1) by pseudo-random permuting the integers from 1 to n_w.
3. Permute the watermark sequence, $\mathbf{u}_w$, based on the sequence of indices obtained from Step 2 to become the scrambled sequence, $\mathbf{u}_p$.
4. Then, rearrange the sequence of $\mathbf{u}_p$ into the two-dimensional $M \times M$ matrix to obtain a permuted image, $\mathbf{W}_p$.

3.2 Spread Spectrum

The pseudo-random (PN) sequence based spread spectrum method [3] is used in our system. SS ensures a large measure of security against various attacks. In the PN-based spread spectrum system, each information bit is expanded into several bits using the PN sequence. To accomplish the job, first $\mathbf{W}_p$ is converted into a bipolar bit sequence, $d(i)$, where $i = 1, 2, \ldots, n_w$ by mapping 0

to 1 and 1 to -1. Second, generate a total of n_w different PN sequences, $p_i(j) \in \{\pm 1\}$, with the same length of l where $j = 1, 2, \ldots, l$ using a user's secret key (which is saved as PN_2 for future watermark detection). By multiplying $d(i)$ with $p_i(j)$, each information-bearing bit is spread into l bits and the whole expanded bipolar bit sequence m is expressed by

$$m_i(j) = d(i) \cdot p_i(j) \tag{14}$$

where $j = 1, 2, \ldots, l$ and $i = 1, 2, \ldots, n_w$.

3.3 Low Amplitude Block Selection

LABS is employed to minimize the difference between the visual qualities of the two images, before and after embedding process as much as possible. The number of transformed 8×8 blocks in the sequency domain is more than the size of spread watermark bit sequence. We sum all the amplitudes in each 8×8 transformed blocks and the LABS strategy selects the 8×8 blocks having lower summations of amplitudes out of the total number of blocks available in order to insert the secret bits. The selection is done over the whole image globally. Consequently, the selected blocks are recorded for future detection purpose using a user's key (which is expressed as Key in Fig. 1).

To make the watermarking scheme robust, the watermark bits should be placed in the most significant components of an image because this portion of the host data is robust to the attacks and highly sensitive to alteration [5]. For most natural images, the energy is concentrated at the lower frequency

range [2,3] and the information hidden in the high or middle frequency bands is easily removed or lost after some operations such as low pass filtering and quantization of lossy compression. Therefore, we embed the secret bits in the lower sequency components in our scheme using the analogy with the frequency-based watermarking scheme. We select $B(1,1)$ as the location to embed the secret bit, which is shown in Fig. 3. The amplitude and phase of $B(1,1)$ are denoted as A and ϕ respectively as mentioned in Fig. 1.

3.4 Amplitude Boost

The purpose of amplitude boost (AB) strategy is to enhance the robustness. In our PSK modulation, the watermark information is inserted into the phases of the selected SCHT coefficient. It has been shown that the phase distortion due to an additive Gaussian noise is inversely proportional to the amplitude of the coefficient [1, 5, 6]. Hence, in order to keep the phase distortion below a certain level, the amplitude of the SCHT coefficient should be maintained at one defined level. In this paper, the AB method is hired to reinforce the robustness of our watermarking scheme. In the AB strategy, the amplitude of a selected SCHT coefficient is boosted to a fixed threshold value t if its value is below t. That is,

$$A' = \begin{cases} t, & \text{if } A \leq t \\ A, & \text{if } A > t. \end{cases} \tag{15}$$

We have observed that the SCHT has certain advantages over the DFT (which is employed in [5]) and the UCHT by using the AB skill in image watermark-

ing. To illustrate this, we embed the watermark using the proposed scheme as shown in Fig. 1 utilizing the DFT, the SCHT and the UCHT by varying the values of t. In our scheme, the watermark is embedded in the phases of the transform coefficients, hence, the WHT and the DCT are not considered for comparison as their coefficients are real numbers. Table 1 shows the corresponding peak signal-to-noise ratio (PSNR) values of the SCHT, DFT and UCHT watermarked images with respect to the original image based on the increasing values of t using the PSK modulation for the Lena image. The PSNR values of the SCHT and DFT watermarked images are reduced when the values of t become larger as shown in Table 1 whereas the t values do not affect the PSNR value of the UCHT watermarked image. It can be observed from the table that at any particular value of t, the PSNR value of the SCHT watermarked image is much higher than that of the DFT and UCHT watermarked images. Therefore, we can increase the value of t as large as possible to enhance the robustness for the SCHT watermarked image while maintaining the image quality at one acceptable level.

3.5 PSK Modulation

In the PSK modulation, the phase ϕ is modified into ϕ' according to the following rule:

$$\phi' = \begin{cases} \pi/2, & \text{if } m(r) = 1 \\ 3\pi/2, & \text{if } m(r) = -1. \end{cases} \tag{16}$$

where $m(r)$ is the bipolar spread watermark bit sequence and $r = 1, 2, \ldots, l \times n_w$. The maximum phase perturbation due to PSK modulation is $\pm\pi$. But the visual quality is still preserved in the watermarked image after embedding the watermark as shown in Fig 5.

4 Watermark Detection Algorithm

Fig. 4 shows the flow chart for the watermark extraction process. It should be noted that the original host image and the watermark are not needed during the recovering process. But it is important that the watermark bits are decoded from the same positions where they have been embedded previously. Therefore, the set of secret keys (Key, PN_1, PN_2) used in the embedding process is to be used in the extraction process as well. The steps to extract the watermark are outlined as follows:

1. The watermarked image $\mathbf{R}$ is segmented into the 8×8 non-overlapping blocks and 2-D SCHT is applied on those 8×8 blocks to transform the image $\mathbf{R}$ to $\mathbf{Y}'_R$.
2. The same Key which was used in the embedding process is reused to locate the respective embedded blocks in $\mathbf{Y}'_R$ for PSK demodulation.
3. During the PSK demodulation, the watermark bits $m_R(r)$ are extracted from the phases of the selected SCHT coefficient from the selected blocks in $\mathbf{Y}'_R$.
4. After all the secret bits are decoded, the extracted bipolar bit sequence is despread by the inverse spread spectrum to obtain a contracted bipolar

bit sequence. It is then transformed back to the binary bit sequence by mapping 1 to 0 and -1 to 1 and rearranged into the two-dimensional $M \times M$ image $\mathbf{W}'_R$.

5. Finally, $\mathbf{W}'_R$ is reverse-permuted to get the recovered watermark $\mathbf{W}_R$ according to the predefined pseudo-random sequence PN_1.

Some steps are elaborated further in the following.

4.1 PSK Demodulation

Let ϕ'' be the angle of interest to extract the secret bit. The minimum distance decision rule is applied in the process of PSK demodulation. Hence, $m_R(r)$ is detected as

$$m_R(r) = \begin{cases} 1, & \text{when } |\phi'' - \frac{\pi}{2}| \geq |\phi'' - \frac{3\pi}{2}| \\ -1, & \text{when } |\phi'' - \frac{\pi}{2}| < |\phi'' - \frac{3\pi}{2}| \end{cases} \tag{17}$$

where $r = 1, 2, \ldots, l \times n_w$.

4.2 Inverse Spread Spectrum

After all the secret bits are recovered from the PSK demodulation, ISS is performed to reconstruct the bipolar watermark bit sequence d_R. By using the PN sequences $p_i(j)$ which were used in spreading (generated by PN_2), each bit can be determined from m_R by

$$d_R(i) = \begin{cases} 1\,, & \text{if } \sum_{j=1}^{l} m_{R,i}(j) \cdot p_i(j) \geq 0 \\ -1\,, & \text{if } \sum_{j=1}^{l} m_{R,i}(j) \cdot p_i(j) < 0 \end{cases} \tag{18}$$

where $i = 1, 2, \ldots, n_w$ and $j = 1, 2, \ldots, l$.

5 Experimental Results

In this paper, PSNR is used to measure the degree of transparency of the watermarked image. In our scheme, we use the visually recognizable pattern as the watermark, hence, the observers can compare the extracted watermark with the referenced watermark subjectively. Therefore, a quantity measurement is required to provide an objective judgement for the extracted fidelity. In this paper, we use normalized correlation (NC) [2, 5] as the similarity measurement between the original and recovered watermarks. It is defined as

$$\mathrm{NC} = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{M-1} W(i,j)W_R(i,j)}{\sum_{i=0}^{M-1}\sum_{j=0}^{M-1}[W(i,j)]^2} \tag{19}$$

which is normalized by the energy of the referenced watermark to give unity as peak correlation, where $\mathbf{W}$ and $\mathbf{W}_R$ represent the original watermark and the extracted watermark of size $M \times M$, respectively.

The Lena image is the most frequently used image and a lot of results are available for comparison. Therefore, we use the original grey-scaled Lena image of (512×512) pixels shown in Fig. 5 in order to evaluate our proposed watermarking scheme as compared to the other schemes, and a symbol of star (32×32) pixels shown in Fig. 2 is used as a watermark in our simulation. But we have tested on other standard images using a randomly generated bit string as a watermark, and it is found that the results are consistent. The values of parameters used in this simulation are: $l = 3$ and $t = 30$ for the SCHT watermarked image whereas $t = 12$ for the DFT watermarked images in order to preserve the visual quality of the images since there is tradeoff

between the image quality (PSNR) and the robustness based on the value of t as mentioned in Subsection 3.4. The block size used is 8×8. The length of watermark bit sequence is $n_w = 32 \times 32 = 1024$ and after spreading, it becomes $1024 \times 3 = 3072$. Therefore, LABS selects 3072 blocks from a total of blocks available which is $(512 \times 512) \div (8 \times 8) = 4096$ blocks as one secret bit is inserted into each 8×8 transformed blocks. Fig. 5 shows the original Lena image and the watermarked images using SCHT, DFT and UCHT. The PSNR values of the corresponding watermarked images with respect to the original image are 39.95 dB, 37.72 dB and 26.41 dB respectively. We can see see from the figures that despite the presence of the watermark, the SCHT watermarked image does not contain any visible artifacts as the DFT watermarked image. One could hardly perceive the difference between the original and watermarked images. But the visual degradation occurs in the UCHT watermarked image as shown in Fig. 5-d. Therefore, UCHT is not suitable for inserting watermark in the direct transformed coefficients, whereas the multiresolutional WHT is first used to decompose the host image into pyramid structure before taking UCHT to perform watermarking [12].

Various attacks are considered to demonstrate the robustness of our watermarking scheme where the Lena image is used as the test image again. The robustness of the watermarked image depends directly on the threshold value t used for AB, which in turn influences the visual degradation of the image as illustrated in Table 1. Attacks include scaling, rotating, cropping, paint-

ing, low-pass filtering, sharpening, nosing, phase perturbation [14] and JPEG compression. The details of each attack are shown below.

(a) Image resizing: The watermarked image is scaled down from its original size of 512×512 pixels to 192×192 pixels. Then the reduced image is re-scaled back to the original dimension before the extraction process.

(b) Image rotation: The image is rotated 90° clockwise followed by 90° anti-clockwise before proceeding the decoding process.

(c) Image cropping I: For the cropping attack I, a quarter of the embedded image is discarded after the cropping operation.

(d) Image cropping II: For the cropping attack II, only the central required portion of the marked image (56.25% of the original size) is remained. In order to extract the watermark, the missing portions are replaced with the black-colored pixels which are zeros. It is shown in Fig. 6-d.

(e) Painting: Several paints are added to the watermarked Lena image as shown in Fig. 6-e.

(f) Low-pass filtering: The filter is a rotationally symmetric Gaussian lowpass filter of the size 3×3 with the standard deviation σ of 1.4. The embedded image is filtered before proceeding the detection process.

(g) Sharpening: The contrast of the image is adjusted to enhance the image quality before extracting the watermark. The sharpened version of the image is shown in Fig. 6-g.

(h) Noising: Gaussian noises with zero mean and normalized variance 0.01 are introduced to the marked image. The noisy version of the watermarked Lena image is shown in Fig. 6-h.

(i) Phase perturbation: As mentioned in [14], first, a normally distributed noise with mean $\pi/4$ and variance 0.01 is generated and then the noise is added to all the middle sequency and high sequency phases of the SCHT coefficients in the sequency domain.

The figures for the corresponding attacked SCHT watermarked images under various kinds of image signal operations are illustrated in Fig. 6. Fig. 7 shows their respective extracted watermarks using the proposed scheme for the Lena image. The corresponding NC values (together with the number of error bits) for each attacked SCHT watermarked image are shown in Table 2 as compared with the results for the attacked DFT watermarked image. It can be seen from Table 2 that for the attacks of rotating, sharpening and phase perturbation, the watermarks are fully recovered from the embedded images as the value of NC is 1 and the number of errors is zero. The NC values which are relevant to the other attacks are also above 0.84 (acceptable number of error bits) and the corresponding extracted watermarks are visually recognized by the human vision as shown in Fig. 7. But it has been observed that for the attack of scaling, more significant error bits are introduced for the SCHT based scheme as compared to the DFT based scheme as shown in Table 2. We have known that re-scaling the image in fact introduces high frequency components in the frequency domain while weakening the low and middle fre-

quency components of the image. Since the watermark bits are embedded in the phases of low frequency/sequency components of the image, re-scaling will lead to corruption of the watermark inserted in the phase domain. As a result, the error bits are detected when the watermark bits are decoded from the re-scaled DFT and SCHT watermarked images as shown in Item (a) of Table 2. But it should be noted that the effect of re-scaling changes mostly the phase angles of the SCHT coefficients in the sequency domain rather than that of the DFT coefficients in the frequency domain.

For the JPEG compression attacks, the watermarked image is compressed using the standard JPEG encoding at various quality levels. Table 3 summarizes the results for JPEG lossy compression tests from 10% to 100% quality factor using the proposed scheme based on both SCHT and DFT. It can be seen from Table 3 that as the quality level decreases, the NC value reduces accordingly. Fig. 8 shows the extracted watermarks from the JPEG compressed versions of the watermarked Lena image based on the SCHT at quality levels 50%, 40%, 30% and 21%. Fig. 9 shows the corresponding decoded watermarks for the DFT based scheme. At 21% quality level, the NC value (which is 0.8) is still high enough to recognize the extracted watermark as shown in Fig. 8-d for the SCHT based scheme. The watermark is visible and we are still able to recover it. But for the DFT based scheme, the extracted watermark is hard to visualize at 21% quality level as shown in Fig. 9-d since the number of error bits is 293, and the NC value is also 0.72 which is lower than that of the SCHT based scheme. It should be noted that below 21%, the qualities of the JPEG

encoded watermarked images for both schemes are degraded severely and the extracted watermarks will become indiscernible.

5.1 Comparison between the SCHT and DFT based watermarking schemes

The comparison of the NC values between the proposed methods using the SCHT and the DFT is listed in Tables 2 and 3. It can be seen from Table 2 that the NC values for both schemes are close to each other under various kinds of attacks and they are all above 0.84. The extracted watermarks are also clearly identified by the human perception as shown in Fig. 7. For the JPEG compression attacks, the scheme using the SCHT is able to provide higher NC values (less number of error bits detected) than that utilizing the DFT from 30% quality level onwards as shown in Table 3. This indicates that the SCHT based watermarking scheme is more robust to the JPEG lossy compression than the DFT based scheme. Besides, the PSNR value of the SCHT watermarked image (which is 39.95 dB) is even higher than the corresponding value of the DFT watermarked image (which is 37.72 dB) as shown in Fig. 5.

Another obvious advantage of the SCHT based scheme over the DFT based scheme is the reduced computational complexity which will lead to consequent hardware savings. In order to compute an 8-point SCHT, the fast algorithm requires 24 complex addition/subtractions [16]. It is similar to that of the radix-2 FFT algorithm to compute an 8-point DFT [19]. But two complex multiplications with the twiddle factors (i.e., W_8^1 and W_8^3 where $W_N^{nk} = \exp(-j\frac{2\pi nk}{N})$) are necessary to perform the 8-point DFT operation but

it is not needed in the computation of the SCHT. For example, if an image of 512×512 pixels is considered for image watermarking, the total number of blocks will be $(512 \times 512) \div (8 \times 8) = 4096$ and each block requires 16 transformations (8-point transforms) using (10). Therefore, an additional saving of $2 \times 16 \times 4096 = 131072$ complex multiplications can be obtained in watermark embedding by using the SCHT as compared to the DFT. This will in turn reduce the hardware requirement (the multipliers) when we actually implement it in the hardware. The same is applied to watermark extraction as well. This is really significant especially for real-time applications. Therefore, the DFT can may replaced with the SCHT for such applications with simpler implementation and consequent savings in computational cost.

In this paper, other than the smooth Lena image, the numerical results are presented for the Barbara image which contains high frequency components as well. The randomly generated bit string is used as a watermark. Tables 4 and 5 summarize the comparisons for the corresponding attacks using the Barbara image. The PSNR value of the SCHT watermarked image with respect to the original image is 39.55 dB whereas it is 36.23 dB for the DFT watermarked image. We have observed from the tables that the results are consistent with previous findings concluded for the Lena image.

5.2 Comparison with the Chen's scheme

Table 6 presents the comparison of robustness of our proposed scheme as compared with the Chen's scheme [5] under various image manipulation attacks.

The watermarking was also performed in the phase domain of the DFT coefficients using the DFT in the Chen's scheme. The Lena image was used in the simulation of the Chen's scheme and the watermark symbol is also the size of (32×32) pixels which is similar to that of our scheme. As shown in Table 6, both schemes are able to sustain different attacks such as resizing, rotating, image cropping, painting and blurring. But the Chen's scheme is vulnerable to the phase perturbation attack which is mentioned in [14] whereas our scheme is able to withstand such attack. In addition, the PSNR value of the SCHT watermarked image with respect to the original image is 39.95 dB, which is larger than the corresponding value in [5], which is 35.34 dB for the Lena image. Besides, it should be noted that the advantage in terms of computational complexity (mentioned in Subsection 5.1) is also applied in this comparison since the Chen's scheme employed the DFT for transformation whereas our scheme used the SCHT.

5.3 Comparison with the Guo's scheme

In [1], Guo et al. introduced the discrete fractional random transform (DFRNT) to develop a novel watermarking algorithm. In this scheme, the phases of the selected transform coefficients were marked using the PSK modulation based on the inserted bits. The test image considered was the Lena image and a watermark symbol of (32×32) pixels was used in the simulation as well. The mean square error (MSE) was used to measure the similarity between the original and extracted watermarks. Table 7 shows the comparison of the MSE

values between our scheme and the Guo's scheme [1] under different kinds of attacks such as cropping, noising and low-pass filtering. The results reveal that our proposed scheme is able to provide smaller MSE values than those of the Guo's scheme, and the differences are also significant for each attack as shown in the table. But it should be noted that the kernel transform matrix of the DFRNT used in the Guo's scheme is random, hence, it provides higher security for the watermarking scheme as compared to our scheme.

5.4 Comparison with the Falkowski's scheme

Table 8 lists the results for the comparison of robustness of our scheme with the Falkowski's scheme [12]. In this scheme, the host image was first decomposed using the multiresolutional WHT in order to identify the most significant components of the image. Then, the multi-polarity complex Hadamard transform (CHT) was performed on the segmented 8×8 blocks of the lowest frequency bank (LSB). The phases of the selected CHT coefficients were altered to convey the watermark sequence. The Lena image was used in that paper and the watermark is a pseudo-random sequence of length 16. As shown in Table 8, both schemes are able to sustain various kinds of image attacks. It is found that the Falkowski's scheme shows better robustness to the JPEG compression attacks (up to 10% quality factor) than our scheme (up to 20% quality factor).

On the other hand, the Falkowski's scheme requires two transformations (i.e., the WHT and the CHT) in order to insert the watermark. But our scheme needs only one transformation (i.e., the SCHT) and the most significant

components of an image are easily determined by the sequency property for watermark insertion. As a result, our scheme requires less computational cost and simpler implementation as compared to the Falkowski's scheme, which can be a better choice for real-time applications. Besides, the watermark which is used by our scheme is visually recognizable and can be easily identified by human perception. The original image is also not needed during the watermark extraction process. But it should be noted that the Falkowski's scheme provides higher PSNR value (which is 41.34 dB) of the watermarked image with respect to the original image than our scheme (where the PSNR value is 39.95 dB).

6 Conclusion

A robust watermarking scheme for grey-scaled images using the sequency-ordered complex Hadamard transform is developed in this paper. Low amplitude block selection is performed on the whole image to improve the image quality of the watermarked image whereas the amplitude boost method is used to enhance the resistance to several attacks. The watermark is embedded into the host image using the PSK modulation in the sequency domain. By using the analogy of sequency with frequency, the watermark bits are inserted into the lower sequency components of the image, which are most significant to the image integrity. The numerical results show that the proposed scheme is robust to various kinds of attacks such as JPEG lossy compression, scaling, rotating, cropping, painting, low-pass filtering, sharpening, noising and phase perturbation attack. Compared to the Chen's scheme, our scheme is able to

provide higher PSNR value of the watermarked image with respect to the original image. In addition, it can also sustain the phase perturbation attack which is described in [14] while maintaining the visual quality of the attacked image at an acceptable level as shown in Fig. 6-i. It is also observed that the proposed scheme performs better than the Guo's scheme in terms of MSE values as shown in Table 7. As compared to the Falkowski's scheme, the proposed scheme has demonstrated similar robustness to various image attacks but it can be considered as a better scheme for real-time applications due to reduced computational cost. Comparison between the proposed methods using the SCHT and the DFT shows that the SCHT can be considered as a good candidate to replace the DFT for such applications. In terms of computational complexity and implementation, the SCHT is much faster and simpler than the DFT with the availability of its fast algorithm and pipelined hardware structure [16]. Therefore, together with the supporting numerical results, it is demonstrated that the SCHT can be considered as a potential and useful tool for digital watermarking applications.

References

1. J. Guo, Z. Liu, and S. Liu, "Watermarking based on discrete fractional random transform," *Optics Communications*, vol. 272, no. 2, pp. 344–348, 2007.
2. C. T. Hsu and J. L. Wu, "Hidden digital watermarks in images," *IEEE Transactions on Image Processing*, vol. 8, no. 1, pp. 58–68, 1999.
3. I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp.

1673–87, 1997.

4. J. J. K. Ó Ruanaidh, W. J. Dowling, and F. M. Boland, "Watermarking digital images for copyright protection," in *IEE Proceedings-Vision, Image and Signal Processing*, vol. 143, no. 4, 1996, pp. 250–6.
5. W. Y. Chen and C. H. Chen, "A robust watermarking scheme using phase shift keying with the combination of amplitude boost and low amplitude block selection," *Pattern Recognition*, vol. 38, no. 4, pp. 587–598, 2005.
6. J. J. K. Ó Ruanaidh, W. J. Dowling, and F. M. Boland, "Phase watermarking of digital images," in *Proc. IEEE International Conference on Image Processing*, vol. 3, 1996, pp. 239–242.
7. X. Qi and J. Qi, "A robust content-based digital image watermarking scheme," *Signal Processing*, vol. 87, no. 6, pp. 1264–80, 2007.
8. R. C. Gonzalez and R. E. Woods, *Digital image processing*, International ed. Pearson Prentice Hall, 2002.
9. M. J. Tsai, K. Y. Yu, and Y. Z. Chen, "Joint wavelet and spatial transformation for digital watermarking," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 241–245, 2000.
10. P. Bao and M. Xiaohu, "Image adaptive watermarking using wavelet domain singular value decomposition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 15, no. 1, pp. 96–102, 2005.
11. F. Fonda and S. Pastore, "Innovative image watermarking technique for image authentication in surveillance applications," ser. Proc. IEEE International Workshop on Imaging Systems and Techniques, Niagara Falls, Ont., Canada, 2005, pp. 32–35.
12. B. J. Falkowski, "Phase watermarking algorithm using hybrid multi-polarity Hadamard transform," *Journal of Mathematical Imaging and Vision*, vol. 30, no. 1, pp. 13–21, 2008.
13. B. J. Falkowski and L. S. Lim, "Image watermarking using the complex Hadamard transform," in *Proc. IEEE International Symposium on Circuits and Systems*, vol. 4, 2000, pp. 573–576.

14. J. S. Pan and C. Lin, "Attacking phase shift keying based watermarking," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E90A, no. 1, pp. 305–6, 2007.

15. A. Aung, B. P. Ng, and S. Rahardja, "Sequency-ordered complex Hadamard transform: Properties, computational complexity and applications," *IEEE Trans. Signal Process.*, vol. 56, no. 8, pp. 3562–3571.

16. G. Bi, A. Aung, and B. P. Ng, "Pipelined hardware structure for sequency-ordered complex Hadamard transform," *IEEE Signal Processing Letters*, vol. 15, pp. 401–404, 2008.

17. A. Aung, B. P. Ng, and S. Rahardja, "Performance of SCHT sequences in asynchronous CDMA system," *IEEE Communications Letters*, vol. 11, no. 8, pp. 641–643, 2007.

18. K. G. Beauchamp, *Applications of Walsh and related functions, with an introduction to sequency theory.* Academic Press, 1984.

19. S. Kuo and W. S. Gan, *Digital signal processors: Architectures, implementations, and applications*, international ed. Pearson Prentice Hall, 2005.

Table 1: The PSNR values of the SCHT and DFT watermarked Lena images arranged according to the ascending threshold values of t

t		12	16	20	24	28	32
PSNR (dB)	SCHT	44.31	43.45	42.41	41.45	40.46	39.58
	DFT	37.72	36.91	36.02	35.11	34.20	33.34
	UCHT	26.41	26.41	26.41	26.41	26.41	26.41

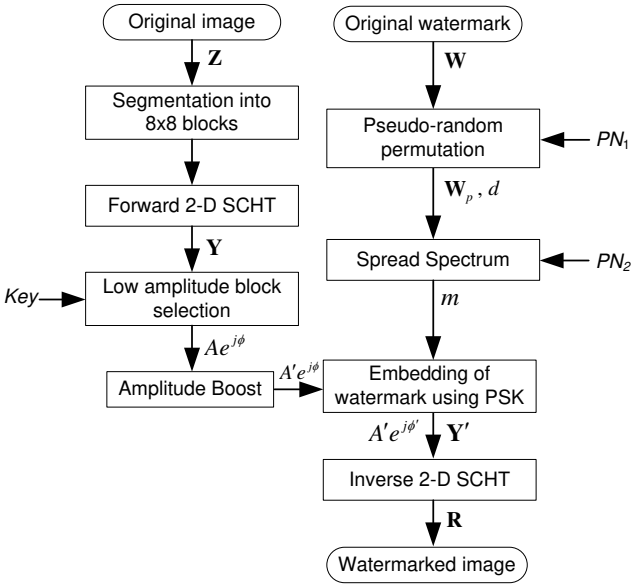

Fig. 1: The flow chart of watermark embedding process.

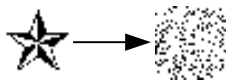

Fig. 2: The watermark transformed by random permutation, (a) the original watermark, and (b) the permuted watermark.

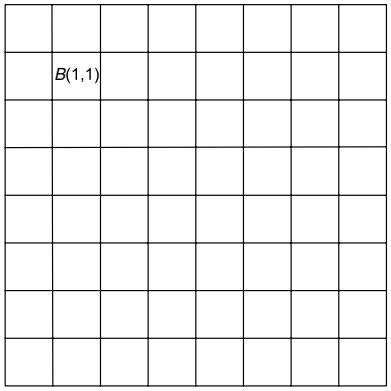

Fig. 3: The selected SCHT coefficient to embed the watermark within a 8×8 block.

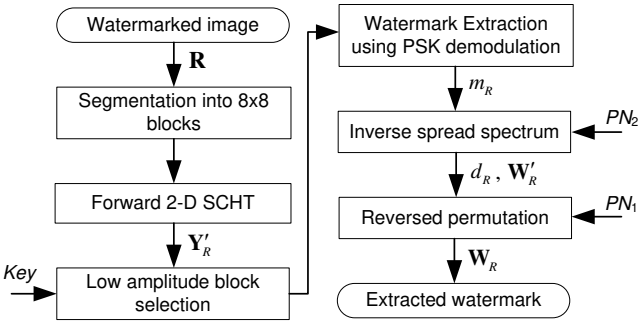

Fig. 4: The flow chart of watermark detection.

Fig. 5: (a) The original image of Lena, the watermarked images of Lena using (b) SCHT with PSNR = 39.95 dB, (c) DFT with PSNR = 37.72 dB, and (d) UCHT with PSNR = 26.41 dB.

Fig. 6: The SCHT watermarked images subjected to various attacks: (a) The resized, (b) the rotated, (c) the cropped (a quarter image), (d) the cropped (central portion remained), (e) the painted, (f) the filtered, (g) the sharpened, (h) the noised, and (i) the phase perturbation attacked.

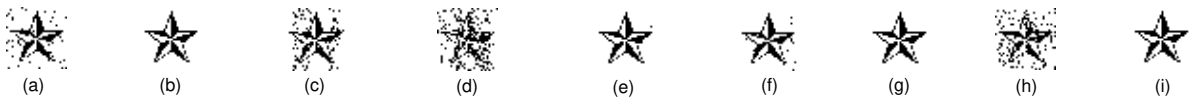

Fig. 7: The corresponding extracted watermarks: (a) The resized, (b) the rotated, (c) the cropped (a quarter image), (d) the cropped (central portion remained), (e) the painted, (f) the filtered, (g) the sharpened, (h) the noised, and (i) the phase perturbation attacked.

Fig. 8: The extracted watermarks from JPEG encoded versions of the SCHT watermarked Lena image (a) at 50% quality with NC≅ 1.00, (b) at 40% quality with NC≅ 1.00, (c) at 30% quality with NC=0.98, and (d) at 21% quality with NC=0.80.

Fig. 9: The extracted watermarks from JPEG encoded versions of the DFT watermarked Lena image (a) at 50% quality with NC≅ 1.00, (b) at 40% quality with NC≅ 1.00, (c) at 30% quality with NC=0.87, and (d) at 21% quality with NC=0.72.

Table 2: Comparison of the NC values corresponding to the number of error bits for the attacked watermarked Lena images under various operations between the SCHT and the DFT based schemes

Attack type	Parameters	SCHT		DFT	
		eBits[a]	NC	eBits[a]	NC
(a) Scaling	512×512 to 192×192	45	0.95	4	0.99
(b) Rotating	90° rotated clockwise	0	1.00	0	1.00
(c) Cropping I	Cropping 1/4	76	0.92	79	0.92
(d) Cropping II	Central portion remained	164	0.84	155	0.85
(e) Painting	Painting 3 bars	2	0.99	2	0.99
(f) Filtering	Size $3 \times 3, \sigma = 1.4$	14	0.99	0	1.00
(g) Sharpening	Sharpening the image	0	1.00	0	1.00
(h) Noising	Gaussian noise added	123	0.88	133	0.87
(i) Phase perturbation	Mean=$\pi/4$, var=0.01	0	1.00	0	1.00

[a] The number of error bits detected.

Table 3: Comparison of the NC values corresponding to the number of errors for the JPEG compressed watermarked Lena images between the SCHT and DFT based schemes

JPEG quality level(%)	SCHT		DFT	
	eBits[a]	NC	eBits[a]	NC
100	0	1.00	0	1.00
90	0	1.00	0	1.00
80	0	1.00	0	1.00
70	1	0.99	0	1.00
60	2	0.99	0	1.00
50	2	0.99	0	1.00
40	2	0.99	11	0.99
30	18	0.98	135	0.87
21	203	0.80	293	0.72
20	228	0.78	304	0.71
10	445	0.56	433	0.58

[a] The number of error bits detected.

Table 4: Comparison between the SCHT and DFT based schemes for various attacks using the Barbara image

Attack type	Parameters	SCHT		DFT	
		eBits[a]	NC	eBits[a]	NC
(a) Scaling	512×512 to 192×192	104	0.91	22	0.98
(b) Rotating	90° rotated clockwise	0	1.00	0	1.00
(c) Cropping I	Cropping 1/4	63	0.94	60	0.94
(d) Cropping II	Central portion remained	135	0.86	124	0.88
(e) Painting	Painting 3 bars	7	0.99	2	0.99
(f) Filtering	Size $3 \times 3, \sigma = 1.4$	21	0.98	0	1.00
(g) Sharpening	Sharpening the image	0	1.00	0	1.00
(h) Noising	Gaussian noise added	136	0.85	133	0.87
(i) Phase perturbation	Mean=$\pi/4$, var=0.01	0	1.00	0	1.00

[a] The number of error bits detected.

Table 5: Comparison between the SCHT and DFT based schemes for the JPEG compressed Barbara image

JPEG quality level(%)	SCHT		DFT	
	eBits[a]	NC	eBits[a]	NC
100	0	1.00	0	1.00
90	0	1.00	0	1.00
80	1	0.99	0	1.00
70	1	0.99	0	1.00
60	2	0.99	0	1.00
50	7	0.99	0	1.00
40	7	0.99	7	0.99
30	23	0.98	80	0.92
21	157	0.85	215	0.78
20	185	0.82	244	0.75
10	417	0.58	399	0.61

[a] The number of error bits detected.

Table 6: Performance comparison between the proposed scheme and the Chen's scheme under different image manipulation attacks for the Lena image

Attack item	Our scheme	The Chen's scheme [5]
Scaling	Pass	Pass
Rotating	Pass	Pass
Cropping I	Pass	Pass
Painting	Pass	Pass
Blurring	Pass	Pass
Phase perturbation [14]	Pass	Fail

Table 7: Comparison of MSE values between the proposed scheme and the Guo's scheme under different kinds of attacks for the Lena image

Attack category	Our scheme	The Guo's scheme [1]
Cropping 1/4	0.0902	0.5970
Cropping 1/16	0.0083	0.4160
Noising $\sigma = 43.39$	0.2550	0.7530
$\sigma = 36.16$	0.2384	0.6930
$\sigma = 28.93$	0.1590	0.5820
$\sigma = 21.69$	0.1008	0.4550
$\sigma = 14.46$	0.0297	0.3230
$\sigma = 7.23$	0.0000	0.1840
Low-pass filtering, [4 4][a]	0.0166	0.2940
[3 3][b]	0.0024	0.1130

[a] Filter size 4×4.

[b] Filter size 3×3.

Table 8: Performance comparison between the proposed scheme and the Falkowski's scheme under various kinds of image attacks for the Lena image

Attack category	Our scheme	The Falkowski's scheme [12]
Image scaling	Pass	Pass
Sharpening	Pass	Pass
Cropping I	Pass	Pass
Noising	Pass	Pass
JPEG Compression	Pass (up to 20% quality factor)	Pass (up to 10% quality factor)